Dictamen en relació amb la consulta del president del Comitè de Personal d'un Ajuntament, en relació amb la confidencialitat de les contrasenyes de correu electrònic.

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit del president del Comitè de Personal d'un Ajuntament, en el que es demana el parer de l'Autoritat en relació amb la confidencialitat de les contrasenyes del correu electrònic, a arrel d'una queixa presentada pel propi representant del Comitè de Personal a l'Ajuntament i de la resposta que se li dóna des de l'Ajuntament.

En el mateix escrit del president del Comitè de Personal es planteja a l'Autoritat una altra consulta, relativa a la comunicació de determinades informacions sobre els treballadors de l'Ajuntament. Atès que aquesta consulta es refereix a una qüestió diferent, s'analitzarà en un informe específic (CNS 14/2012).

Analitzada la petició i la normativa vigent aplicable, i vist l'informe de l'Assessoria Jurídica, es dictamina el següent:

I

(...)

II

El president del Comitè de Personal explica que es fa queixar (a l'Ajuntament) que el seu correu electrònic tenia una contrasenya assignada per la persona que porta la gestió informàtica de l'Ajuntament, cosa que al seu parer no reunia la confidencialitat que li atorga la LOPD. En resposta a aquesta queixa la persona que formula la consulta va rebre un correu electrònic -que s'adjunta a l'escrit de consulta-, en el qual s'explica que la contrasenya del correu corporatiu de l'Ajuntament, "l'heu pogut canviar en qualsevol moment" mitjançant el servei de webmail de l'Ajuntament. En aquest mateix correu electrònic s'afegeix que l'usuari té l'opció de canviar la contrasenya tantes vegades com es vulgui a la mateixa web i fins al març de 2011, moment en el qual, per raons tècniques (canvi de la interfície de webmail i de l'empresa que gestiona el servei), el sistema per canviar la contrasenya canvia. A partir d'aquest moment, segons s'explica en el citat correu electrònic, el sistema de canvi de contrasenya consisteix en escriure (des de l'adreça de l'usuari) un correu electrònic a una adreça determinada, "i allà envieu la contrasenya actual i la nova que es vol". La resposta a la queixa conclou afirmant que ambdós processos (de canvi de contrasenya), tant l'antic com el nou, tenen completa confidencialitat.

El representant del Comitè de Personal, disconforme amb la resposta rebuda, considera que l'opció actual de canvi de contrasenya no acompleix la confidencialitat que cal per ajustar-se a la LOPD. Per això sol·licita **"Saber si és correcte la manera de gestionar les contrasenyes del correu electrònic o per contrari vulnera la LOPD."**

Vistos els termes de la consulta, es recorda que la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (en endavant, LOPD) defineix les dades de caràcter personal com "qualsevol informació referent a persones físiques identificades o identificables" (art. 3.a) de la LOPD). L'article 5.1.f) del Reial decret

1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la LOPD (en endavant, RLOPD) afegeix que és dada de caràcter personal "qualsevol informació numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus que concerneix persones físiques identificades o identificables".

Segons el RLOPD, és *identificable*, "qualsevol persona la identitat de la qual es pugui determinar, directament o indirectament, mitjançant qualsevol informació referida a la seva identitat física, fisiològica, psíquica, econòmica, cultural o social. Una persona física no es considera identificable si la dita identificació requereix terminis o activitats desproporcionats" (article 5.1.o) del RLOPD).

Cal tenir en compte que una adreça de correu electrònic apareix necessàriament vinculada a un domini concret, de tal manera que és possible procedir a la identificació del seu titular mitjançant la consulta del servidor en què es gestioni aquest domini, sense que això requereixi un esforç desproporcionat per part de qui procedeix a la identificació. A més, les adreces de correu electrònic dels treballadors, en aquest cas, d'un Ajuntament, és probable que es configurin de tal manera (nom del treballador@nom del domini) que fàcilment permetin identificar als seus titulars.

D'entrada, és clar que la informació relativa a l'adreça de correu electrònic dels treballadors, en aquest cas, d'un Ajuntament –en concret, de la persona que formula la consulta-, es pot qualificar com a dada personal. Per tant, el *tractament* d'aquesta informació personal (article 3.c) de la LOPD), s'ha de sotmetre als principis i obligacions de la normativa en matèria de protecció de dades.

Ara bé, en el cas que ens ocupa, cal partir de la base que l'aplicació dels principis i les garanties de la normativa de protecció de dades no protegeix, només, les adreces de correu electrònic -que per altra banda són dades personals que poden ser habitualment i fàcilment conegudes per terceres persones-, sinó també a la resta d'informació personal que pugui contenir-se en els missatges de correu electrònic. La LOPD protegeix, per tant, tota aquella informació personal del treballador usuari de l'adreça de correu electrònic, i també de qualsevol altra persona física, la informació de la qual pugui contenir-se en els dits missatges.

III

Aquesta Autoritat ha analitzat en diversos Dictàmens les obligacions que la LOPD imposa als responsables del tractament de dades personals en relació amb l'aplicació de mesures de seguretat. En concret, s'han examinat qüestions relatives a la identificació i l'autenticació d'usuaris (Dictàmens 21/2008, 28/2011 i 4/2012), així com diverses qüestions relatives a l'ús dels sistemes i tecnologies de la informació i la comunicació per part del personal al servei d'un Ajuntament (Dictamen 17/2009), entre d'altres qüestions. Aquests dictàmens es poden consultar a la pàgina web: www.apd.cat.

Per situar la qüestió que ens ocupa, cal recordar que l'article 9 de la LOPD estableix l'obligació, per als responsables dels fitxers o tractaments, en aquest cas, l'Ajuntament, d'aplicar una sèrie de mesures de seguretat. L'apartat 1 d'aquest article disposa que:

> *"El responsable del fitxer i, si s'escau, l'encarregat del tractament han d'adoptar les mesures de caràcter tècnic i organitzatiu necessàries que garanteixin la seguretat de les dades de caràcter personal i n'evitin l'alteració, la pèrdua, el tractament o l'accés no autoritzat, tenint en compte l'estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos a què estan exposats, tant si provenen de l'acció humana o del medi físic o natural."*

Les mesures de seguretat que són exigibles als fitxers i tractaments de dades de caràcter personal es classifiquen en tres nivells: bàsic, mitjà i alt, i en el Títol VIII del RLOPD es concreten les mesures tècniques i organitzatives que corresponen a cada nivell. En concret, l'article 81 precisa els nivells de seguretat que caldrà adoptar, en atenció a les categories de les dades personals tractades, de la finalitat del fitxer o tractament, i de que aquests fitxers i tractaments siguin manuals o automatitzats. El Títol VIII del RLOPD també concreta que caldrà consignar les corresponents mesures en el document de seguretat (article 88).

L'Ajuntament ha d'articular una sèrie de mesures que es refereixen, entre d'altres, al control d'accessos per part dels *usuaris* – entre d'altres, els seus propis treballadors, als efectes que interessen en relació amb la consulta formulada-, als recursos necessaris per exercir les seves funcions, a mesures que garanteixin la correcta identificació i autenticació dels usuaris, o a diverses mesures en relació amb la gestió de suports i documents. Algunes d'aquestes mesures impliquen, per exemple, que el responsable hagi d'implementar sistemes que permetin l'autenticació, és a dir, la comprovació de la identitat d'un usuari, a través d'una contrasenya o d'altres sistemes, si escau, o que hagi de comprovar quins són els accessos autoritzats a determinada informació, és a dir, conèixer i establir quines són les autoritzacions que cal concedir a cada usuari en relació amb la utilització de diversos recursos o informacions. També cal habilitar un procediment de notificació i gestió de les incidències que afectin les dades de caràcter personal i s'ha d'establir un registre en què es faci constar el tipus d'incidència, el moment en què s'ha produït, o si s'escau, detectat, la persona que fa la notificació, a qui se li comunica, els efectes que se'n deriven i les mesures correctores aplicades.

En concret, als efectes que ara interessen, en el marc de les mesures de seguretat que l'Ajuntament ha d'aplicar en relació amb la gestió de les adreces de correu electrònic dels seus treballadors, cal fer especial esment a la identificació i l'autenticació dels usuaris, en aquest cas, els propis treballadors de l'Ajuntament.

Segons disposa l'article 93 del RLOPD:

> *"1. El responsable del fitxer o tractament ha d'adoptar les mesures que garanteixin la **correcta identificació i autenticació dels usuaris**.*
> *2. El responsable del fitxer o tractament ha d'establir un mecanisme que permeti la identificació de forma inequívoca i personalitzada de qualsevol usuari que intenti accedir al sistema d'informació i la verificació conforme està autoritzat.*
> *3. Quan el mecanisme d'autenticació es basi en **l'existència de contrasenyes**, hi ha d'haver un procediment d'assignació, distribució i emmagatzematge que en garanteixi la **confidencialitat** i integritat.*
> *4. El document de seguretat ha d'establir la periodicitat, que en cap cas ha de ser superior a un any, amb què s'han de canviar les contrasenyes que, mentre estiguin vigents, s'han d'emmagatzemar de forma ininteli·ligible. "*

Cal fer esment que les mesures previstes en els articles 89 a 94 del RLOPD són mesures de nivell bàsic, per tant, són d'obligat compliment en relació amb qualsevol tractament automatitzat de dades personals. Això vol dir que les previsions de l'article 93, esmentat, s'han d'aplicar necessàriament en el cas que ens ocupa. L'Ajuntament, per tant, té l'obligació d'implantar un mecanisme que permeti que la identificació dels usuaris del correu electrònic corporatiu –els propis treballadors-, sigui inequívoca i personalitzada.

El mecanisme d'identificació i d'autenticació triat per l'Ajuntament per a articular l'ús del correu electrònic per part dels seus treballadors, per la informació de què es disposa, inclou efectivament la utilització de contrasenyes, cosa que, en sí mateixa, s'ajusta a les previsions de la normativa de protecció de dades.

Ara bé, cal tenir en compte una sèrie d'exigències que es deriven de les previsions normatives esmentades. En aquest sentit, és necessari que:

- El procediment de gestió de les contrasenyes garanteixi la confidencialitat i la integritat de les mateixes.
- La contrasenya sigui robusta. La major o menor exigència en aquest aspecte dependrà de la naturalesa de la informació protegida, però en qualsevol cas pot portar a establir uns requeriments mínims.
- El responsable estableixi perfils d'usuaris per tal que cada usuari pugui accedir només a aquella informació per a la qual estigui autoritzat.
- Les contrasenyes es canviïn de forma periòdica, i en qualsevol cas sempre abans d'un any.

Es desprèn d'això que als treballadors de l'Ajuntament, en particular, a la persona que formula la consulta, se'ls ha d'atorgar un usuari i una contrasenya "segurs". De l'exigència de confidencialitat es pot inferir que la contrasenya només ha de ser coneguda pel propi interessat, és a dir, pel propi treballador. Lògicament, el coneixement d'una contrasenya per altres persones a banda del propi treballador, invalidaria la necessària confidencialitat de la contrasenya, que perdria la seva funció de permetre l'ús d'un compte de correu electrònic assignat a un treballador, única i exclusivament per part d'aquest treballador.

Per la informació de què es disposa, el sistema d'assignació de la contrasenya utilitzat a l'Ajuntament consisteix en què, quan un treballador disposa d'un compte de correu electrònic corporatiu, se li assigna una primera contrasenya predeterminada que aquest pot canviar. Aquest sistema d'atribució inicial d'una contrasenya en principi no planteja problemes des de la perspectiva de la protecció de dades, sempre i quan el responsable -l'Ajuntament-, adverteixi a l'usuari de la necessitat de canviar la contrasenya assignada inicialment, al més aviat possible, per una altra que només conegui l'usuari.

Diferent valoració ha de merèixer el mecanisme de canvi de contrasenya utilitzat per l'Ajuntament, segons el qual, quan un treballador vol canviar la seva contrasenya, ha d'escriure un correu electrònic amb la contrasenya actual i la nova, i l'ha d'enviar a un tercer (l'empresa que gestiona el servei) per a què aquest tercer efectuï el canvi de contrasenya. Com s'ha apuntat, segons es desprèn de l'explicació de l'Ajuntament, les dues contrasenyes -l'actual i la nova-, s'envien per correu electrònic a una adreça de l'empresa que gestiona actualment el servei.

Respecte d'això, i sens perjudici que, si escau, calgui establir el corresponent encàrrec de tractament de dades personals per part d'aquesta empresa (articles 12 de la LOPD, i 20 a 22 del RLOPD), cal fer avinent que l'enviament de les contrasenyes per correu electrònic permet el coneixement d'aquestes per part d'un nombre indeterminat de persones diferents al propi usuari, cosa que no permet garantir la necessària confidencialitat de la contrasenya. El sistema utilitzat podria arribar a permetre, al menys hipotèticament, un accés i utilització del correu electrònic d'un treballador per part d'un nombre indeterminat de persones, cosa que, precisament, les mesures de seguretat previstes al RLOPD, citat, pretenen evitar.

Per tot l'exposat, cal fer avinent que el sistema de canvi de contrasenyes utilitzat per l'Ajuntament, per la informació de què es disposa, no s'ajusta a les exigències del RLOPD, ja que no permet assegurar la confidencialitat de la contrasenya, en el sentit que només sigui coneguda pel propi usuari, en els termes que exigeix l'article 93 del RLOPD.

D'acord amb les consideracions fetes fins ara, es fan les següents,

Conclusions,

Tant l'adreça de correu electrònic, com la resta d'informació personal dels treballadors d'un Ajuntament i de terceres persones que es pot contenir en els correus electrònics, són dades de caràcter personal. Per tant, el *tractament* d'aquesta informació personal (article 3.c) de la LOPD), s'ha de sotmetre als principis i obligacions de la normativa en matèria de protecció de dades.

El sistema de canvi de contrasenyes de correu electrònic corporatiu utilitzat per l'Ajuntament no s'ajusta a les exigències de la LOPD i el RLOPD, ja que no permet assegurar el correcte compliment de les mesures de seguretat aplicables, en concret, en relació amb la necessària confidencialitat de les contrasenyes.

Des de la perspectiva de la protecció de dades, cal que l'Ajuntament revisi el procediment d'assignació, distribució i emmagatzemament de contrasenyes actual, per tal de garantir-ne la necessària confidencialitat i la integritat, assegurant així el correcte compliment de les mesures de seguretat (especialment, els articles 91 i 93 del RLOPD), i fer-ho constar adequadament al document de seguretat (article 88 del RLOPD).

Barcelona, 10 d'abril de 2012